

POLICY 6.00 SECURITY PATCHES

Software security patches will be installed in an effective and efficient manner.

PURPOSE:

To ensure installed systems contain the latest authentic, tested and approved security patches released to prevent both unintentional and intentional exploitations of information resource process errors and weaknesses.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

OBJECTIVES:

1. Ensure that information technology resources are protected in accordance with the statutes of the State of Tennessee.
2. Ensure the timely installation of the authentic, tested, and approved systems and application security patches.
3. Ensure that all who manage or access information resources employ established State of Tennessee security standards.
4. Promote the safeguarding of information technology resources in a cost effective manner such that the cost of security is commensurate with the value and sensitivity of the resources.

SCOPE:

The policy applies to state agencies, persons or organizations that use, process, or store computerized data relevant to official State of Tennessee business.

IMPLEMENTATION:

Office for Information Resources (OIR)

1. Maintain network infrastructure component software and operating system configurations at the latest release or upgrade level compatible with the State's enterprise environment.
2. Monitor applicable software releases and versions.
3. Ensure supporting documentation is available in a centralized repository.
4. Ensure patch implementations are verified, tested, and approved for deployment.
5. Monitor statewide compliance for deployment of software releases, patches or upgrades.

Agency

1. Ensure that agency managed information resources conform to the latest software release applicable to their environment.
2. Ensure agency managed information assets reflect all appropriate patches.
3. Ensure supporting documentation is available in a centralized repository.
4. Ensure the timely backup of system upgrades and patches.
5. Coordinate networked computer-processing activities with OIR.
6. Adhere to statewide and agency policies, standards, procedures and guidelines ensuring the systems installations maintain the current version, including all tested, and approved security patches.
7. Refrain from implementing agency procedures, processes or practices that would expose networked information resources to unnecessary or unauthorized security risks.
8. Implement no procedure that does not conform to the State security patch installation guidelines without the express written permission of the Office for Information Resources (OIR).

Individual Users/Clients

1. Adhere to statewide and agency policies, standards, procedures and guidelines ensuring the systems installations maintain the current version, including all tested, and approved security patches.
2. Refrain from behaviors that would expose networked information technology resources to unnecessary or unauthorized security risks.